REMARKS

I. General

Claims 1-54 were pending in the present application and were rejected in a Final Office Action (mailed January 6, 2005). The outstanding issues in the Final Office Action are:

- Claims 1, 10, 11, 13-18, 37, 40-47, and 51-54 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,347,374 issued to Drake et al. (hereinafter "*Drake*");

- Claims 2-9, 19-36, 38-39, and 48-50 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Drake* in view of U.S. Patent No. 5,920,719 issued to Sutton et al. (hereinafter "*Sutton*"); and

- Claim 12 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Drake* in view of U.S. Patent No. 6,253,337 issued to Maloney et al. (hereinafter "*Maloney*").

In response, Applicant has filed a request for continued examination (RCE) with this accompanying amendment. Applicant respectfully traverses the outstanding claim rejections, and requests reconsideration and withdrawal thereof in light of the amendments and remarks presented herein.

II. Amendments

Claims 1, 5-7, 14, 15, 20, 21, 23, 26, 27, 31, 36, 37-39, 47 and 54 are amended herein. No new matter is added by these amendments.

Claim 1 is amended to recite that the collected audit data is "raw audit data". Support for this "raw audit data" can be found, *inter alia*, at page 15, line 23 – page 16, line 3 and page 28, lines 24-28 of the present application. Claim 1 is also amended to delete the reference to "a first format" and to "wherein said desired format is different than said first format". These deletions are intended as broadening amendments. Claims 5-7 are amended to recite "raw audit data" for consistency with amended claim 1 from which they each

directly or indirectly depend. Further claim 7 is amended to delete "that is included within said collected audit data", which is intended to be a broadening amendment.

Claim 14 is amended to replace "computer readable" with "computer-readable" in the preamble to correct a typographical error. This amendment is intended to be merely cosmetic and is not intended to alter the scope of the claim in any way. Further, claim 14 is amended to recite "raw" audit data. Claims 15, 21, and 23 are amended to recite "raw" audit data for consistency with amended claim 14 from which they each directly or indirectly depend.

Claim 20 is amended to replace "elements" with "element" to correct a typographical error. This amendment is intended to be merely cosmetic and is not intended to alter the scope of the claim in any way.

Claim 26 is amended to recite "raw" audit data. Claims 28, 31, and 36 are amended to recite "raw" audit data for consistency with amended claim 26 from which they each directly or indirectly depend.

Claim 37 is amended to recite "raw" audit data, and to recite that the raw audit data is "collected by an auditing program". Claims 38 and 39 are amended to recite "raw" audit data for consistency with amended claim 37 from which they each directly or indirectly depend.

Claim 47 is amended to replace the semicolon at its end with a period in order to correct a typographical error. This amendment is made solely for cosmetic purposes and is not intended to change the scope of claim 47 in any way.

Claim 54 is amended to recite "raw" audit data.

III. Rejections under 35 U.S.C. § 102(e) over *Drake*

Claims 1, 10, 11, 13-18, 37, 40-47, and 51-54 were rejected in the Final Office Action under 35 U.S.C. § 102(e) as being anticipated by *Drake*. Applicant respectfully traverses this rejection as provided further below.

To anticipate a claim under 35 U.S.C. § 102, a single reference must teach every element of the claim, *see* M.P.E.P. § 2131. Applicant respectfully submits that *Drake* fails to

teach each and every element of claims 1, 10, 11, 13-18, 37, 40-47, and 51-54, as discussed below.

A. Independent Claims 1, 14, 37, and 54

Drake fails to teach each of the elements of independent claims 1, 14, 37, and 54. For instance, independent claim 1 recites in part "software code executable by at least one processor to receive said raw audit data and generate output comprising at least a portion of said raw audit data in a desired format defined by a template" (emphasis added).

Similarly, independent claim 14 recites in part "code executable to generate output comprising at least a portion of said raw audit data, said output having a format defined by said audit transformation template" (emphasis added).

Independent claim 37 recites in part "function executable to generate output comprising at least a portion of said raw audit data, wherein said output has a format defined by said template" (emphasis added).

Independent claim 54 recites in part "generating said output presentation that includes at least a portion of said raw audit data, wherein said output presentation comprises said desired format as defined by said audit transformation template" (emphasis added).

Drake fails to teach at least the above elements of these independent claims. *Drake* at col. 5, lines 21-32 provides an event detection system:

> which can be viewed as a dual three-tiered implementation with a database 12 in the middle. On one side is an audit analysis engine 14, which converts raw audit data into a standardized format, and performs expert system analysis on the data. On the other side is a user interface 16, which consists of management and control functions, and an application user interface that provides data mining tools to the use of the invention referred to herein as the event detection system.
>
> In *Drake*, events are:
>
> stored in relational database 12 in a normalized format, i.e., standard, that maximizes storage capacity and flexibility. The normalized format also

> simplifies analysis of events, in that no matter what the audit source 18, the events are represented in a single format. Col. 5, lines 62-67.

External to the database 12, events are passed between processes in a standardized representation referred to as a Virtual Record. The Virtual Record is a standardized flat representation of an event in normalized format. Col. 6, lines 4-8. "A parser 20 performs the audit parsing, and has as its sole function the conversion of raw event records into Virtual Records." Col. 7, lines 37-39.

Drake shows in FIG. 1 that a GUI 16 is operable to interact with CMDS database 12 (to which the audit data is stored in a normalized format). For instance, *Drake* provides at column 17, lines 25-59:

> The major functional areas that are addressed by the auditor/investigator GUI are as follows: manual raw audit file management, archive/restore; configure automated audit file archive; and maintenance of an audit file archive database; event detection system user identification and authentication; database connectivity with filter and sort capabilities for selecting and displaying event data in tabular format; an indicator on a tabular GUI display window to indicate when filtering is active; user interface for saving and selecting multiple filter and sort templates (setups) by user defined names (these saved setups are associated with the user, and are available when the user logs in to event detection system); allowing each authenticated user to save a default GUI setup, including the default filter and sort setup; an event status bar for graphical display of the highest event severity level, which has not yet been observed (after the initial observation of an event in the tabular display, the status bar will no longer use that event to update the status bar); user interface allowing the user to mark selected datasets in the database as "responded to" (events that have been responded to, will no longer be displayed in the default event display mode, but may be re-selected for display through a filter); print selected datasets; export selected datasets to a file; display selected datasets in chart form; display the status of distributed event detection system executables; display and print charts, including bar charts (n selected items horizontal, by value vertical, or n selected items horizontal, by m selected items deep, by value vertical from a currently filtered data set); creating chart templates; saving chart templates by name; creating a statistical template for a statistical viewer; saving statistical templates; displaying and printing statistical data, and statistical charts; viewing user status, including login status of user(s), vacation/tagged user status; and default data set filtering for selected users.

While *Drake* mentions use of templates in GUI 16, which retrieves normalized audit data from database 12, *Drake* provides no teaching or suggestion of a template for defining

an output comprising raw audit data. Rather, *Drake* transforms its raw audit data to a normalized format, which is stored to database 12, and the GUI 16 accesses such normalized data rather than the raw audit data.

Accordingly, *Drake* fails to teach at least the above-identified elements of the independent claims 1, 14, 37, and 54.

B. Dependent Claims 10, 11, 13, 15-18, 40-47, and 51-53

Dependent claims 10, 11, 13, 15-18, 40-47, and 51-53 stand rejected under 35 U.S.C. § 102(e) as being anticipated by *Drake*. In view of the above, Applicant respectfully submits that independent claims 1, 14, and 37 are not anticipated by *Drake* because *Drake* fails to teach every element of those independent claims. Further, each of dependent claims 10, 11, 13, 15-18, 40-47, and 51-53 depend either directly or indirectly from one of independent claims 1, 14, and 37 and thus inherit all limitations of the respective independent claim from which they depend. It is respectfully submitted that dependent claims 10, 11, 13, 15-18, 40-47, and 51-53 are allowable not only because of their dependency from their respective independent claims for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compel a broader interpretation of the respective base claim from which they depend).

IV. Rejections Under 35 U.S.C. § 103(a)

Claims 2-9, 19-26, and 38-39 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Drake* in view of *Sutton*. Also, claim 12 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Drake* in view of *Maloney*. Dependent claims 2-9, 19-26, and 38-39 each depend either directly or indirectly from one of independent claims 1, 14, and 37, and thus inherit all limitations of the respective independent claim from which they depend. It is respectfully submitted that dependent claims 2-9, 19-26, and 38-39 are allowable not only because of their dependency from their respective independent claims for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compel a broader interpretation of the respective base claim from which they depend).

Additionally, Applicant respectfully submits that independent claim 26 is not obvious under 35 U.S.C. § 103(a) over *Drake* in view of *Sutton*, as discussed further below. To establish a prima facie case of obviousness, three basic criteria must be met. *See* M.P.E.P. § 2143. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references must teach or suggest all the claim limitations. Without conceding any other criteria, Applicant respectfully asserts that the rejection does not satisfy the third criteria.

Independent claim 26 recites in part "generating an output that includes at least a portion of said raw audit data, wherein said output comprises said desired format as defined by said audit transformation template" (emphasis added). As described above, *Drake* fails to teach or suggest an audit transformation template that defines a desired format for generated output that includes at least a portion of raw audit data. *Sutton* also fails to teach or suggest this element. Accordingly, the applied combination of *Drake* and *Sutton* fails to teach or suggest at least the above element of independent claim 26. As such, independent claim 26 is not obvious under 35 U.S.C. § 103(a) over *Drake* in view of *Sutton*. Therefore, Applicant respectfully requests that this rejection be withdrawn.

Also, dependent claims 27-36 and 48-50 each depend either directly or indirectly from independent claim 26, and thus inherit all limitations of independent claim 26. It is respectfully submitted that dependent claims 27-36 and 48-50 are allowable not only because of their dependency from independent claim 26 for the reasons discussed above, but also in view of their novel claim features.

V. Conclusion

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to pass this application to issue.

Applicant believes no fee is due with this response beyond the fee dealt with in the accompanying Request for Continued Examination Transmittal. However, if an additional fee is due, please charge Deposit Account No. 08-2025, under Order No. 10013502-1 from which the undersigned is authorized to draw.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV 482708426US in an envelope addressed to: M/S RCE, Commissioner for Patents, Alexandria, VA 22313.

Date of Deposit: April 6, 2005

Typed Name: Gail L. Miller

Signature: Gail L. Miller

Respectfully submitted,

By: _____
Jody C. Bishop
Attorney/Agent for Applicant(s)
Reg. No. 44,034
Date: April 6, 2005
Telephone No. (214) 855-8007